

Test Project

Module A1

Assessing security

Cyber Security

Contents

Introduction to Test Project	3
Introduction.....	3
<i>Physical Topology</i>	<i>3</i>
<i>Logical Topology.....</i>	<i>5</i>
Description of project and tasks.....	5
Instructions to the Competitor.....	5
Appendix 1	7
Executive Summary:.....	7
Table 1	7

Introduction to Test Project

You have been asked to assess the security configuration of a website set up on a Linux server using Apache. Your clients are non-technical and hired a consultant to do the configuration of the website settings, but aren't sure of how secure it would be for them to upload their content and put it online. The intention is to have only the members of the webusers group from the domain have access. They are looking for your recommendations in terms of what possible vulnerabilities exist in the system, why these vulnerabilities might be a problem and what they could do to fix the issues.

Login credentials for the competitor Laptops are as follows:

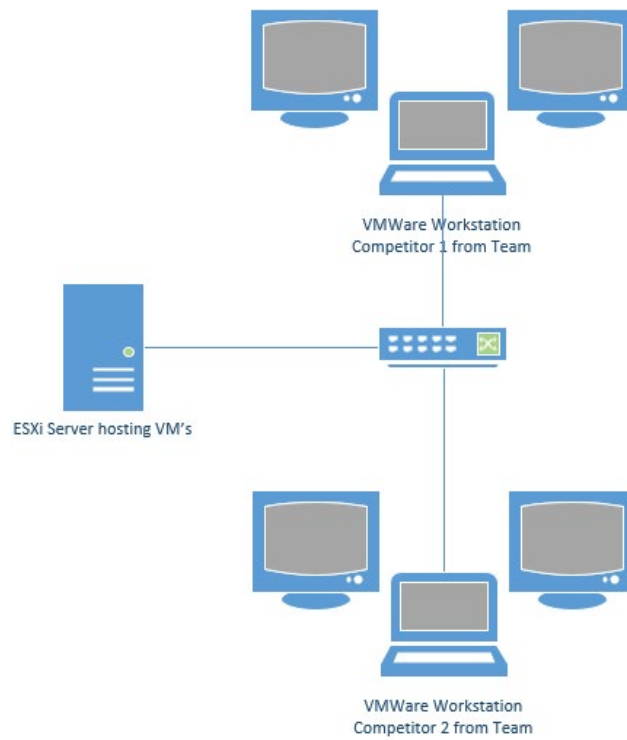
User:**Competitor0**

Password:**CharterDressing**

Introduction

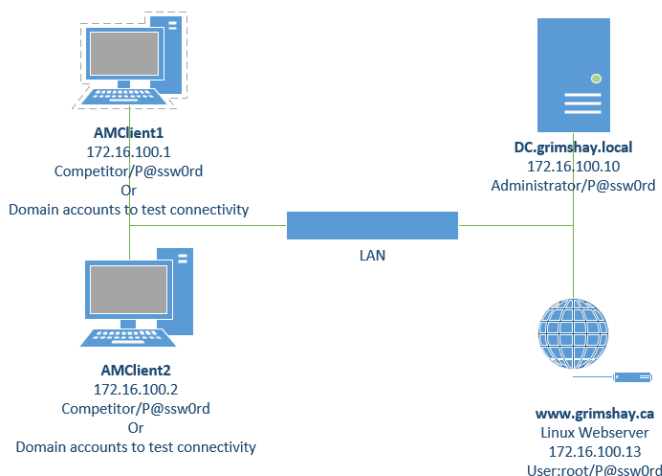
Physical Topology

The physical topology of this project is as follows: competitors from each team will use VMWare Workstation to access VM's hosted on a local ESXi server. All teams will have the same configuration and VM's, but only have access to their own VM's. As per the following diagram:



Logical Topology

The logical topology of the VM's provided on the ESXi server is as follows with the following Network configuration:



Description of project and tasks

This is not a pentest, but an investigation of an existing configuration.

Given the short time frame and lack of Internet connectivity to investigate CV numbers etc., update the appendix of this to document to include:

- An executive summary of your findings on the overall network.
- A documentation of two vulnerabilities found in relation to the website (listed below).

Instructions to the Competitor

All existing user accounts have a password of **P@ssw0rd** including the root and administrator accounts.

We know that this is a weak password to use and have done this for ease of use and assessment at the competition and should not be considered a vulnerability.

All VM's have statically configured IP addresses. You are responsible verifying if these are set correctly in the case that a setting on a virtual machine is different than this document.

The **DC** machine hosts Active Directory, with a number of users and serves as the DNS server for the network.

The **WWW** machine hosts the www.grimshay.ca website to be assessed.

The **AMclient** machines are domain joined and can be used to test access to the website. Chrome, putty, and Wireshark have been installed on the client machines to allow concurrent access and testing from both competitors at the same time. Any existing domain users or the local account can be used to access the client machines.

Examine and familiarize yourself with the Virtual Machines write the executive summary in the appendix. No more than 500 words. You have been directed to assess the security of the Apache installation and website, not other machines or configurations.

For the Apache instance and website, select the two vulnerabilities which in your opinion are the most critical to address. Identify the vulnerabilities associated with that services in the Appendix on Table 1.

- <https://www.grimshay.ca> website on Linux server.

This document will be provided digitally on the Competitor workstation, combine the answer documents to a single file for submission which should be left on desktop of the competitor. When you signal to experts that you are done it will be collected, make sure that you have labelled the file to be saved with your country code, and that experts are able to collect it before you leave.

Log on credentials to the ESXi server are as follows.

IP:**192.168.1.1**

User:**amuser**

Password:**Mt Blanc**

Appendix 1

Executive Summary:

Your text for the executive summary should go here...

Table 1

VULNERABILITY	DESCRIPTION	SEVERITY (0-10)	RISK (LOW/MEDIUM/ HIGH/CRITICAL)	WHY IS THIS A PROBLEM?	RECOMMENDATIONS FOR ACTIONS TO FIX VULNERABILITY
1					
2					